The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
08/28/2012
08/29/2012 - UPDATED

SUBJECT:
Oracle Java Runtime Environment is prone to a remote code execution vulnerability.

OVERVIEW:
A vulnerability has been discovered in Oracle Java Runtime Environment that can lead to remote code execution. The Java Runtime Environment is used to enhance the user experience when visiting web sites and is installed on most desktops and servers. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file.

Please note that there have been reports of active exploitation of this vulnerability and public exploit code is currently available. ***At this time, no patch is available from Oracle to mitigate this vulnerability.***

August 29 – UPDATED OVERVIEW
Please note that the exploit code for this vulnerability has been incorporated into the Blackhole exploit kit which significantly increases the severity of this vulnerability.

SYSTEMS AFFECTED:

- Oracle JRE 1.7.0 Update 6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in Oracle Java Runtime Environment that can lead to remote code execution. In order to exploit this vulnerability, an attacker must first create a malicious web page designed to leverage this issue. When the web page is visited, the attacker-supplied code is run in the context of the affected application.

Please note that there have been reports of active exploitation of this vulnerability and public exploit code is currently available. At this time, no patch is available from Oracle to mitigate this vulnerability.

Initial reports indicate that exploit code is being served from ok.aa24.net / meeting / index.html. The site then loads a Java applet containing the following class files:

- Gondzz.class
- Gondvv.class

The applet then checked to see if the system is vulnerable and downloads the following file:

ok.aa24.net / meeting / hi.exe

This file appears to be a variant of the Poison Ivy malware.

When executed, the file connects to hello.icon.pk (223.25.233.244) over port 80/TCP.

Please note that this is only one reported scenario and the exploit may be delivered via any specially crafted website and could subsequently reach out to any other system after the initial exploitation.

August 29 – UPDATED DESCRIPTION
Please note that the exploit code for this vulnerability has been incorporated into the Blackhole exploit kit which significantly increases the severity of this vulnerability.

RECOMMENDATIONS:

- Apply the patch from Oracle, after appropriate testing, as soon as one becomes available.
- Consider disabling Java completely on all systems until a patch is available.
- Block all traffic to the systems identified in this advisory.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources

REFERENCES:
SecurityFocus
http://www.securityfocus.com/bid/55213

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681

ZDNet
http://www.zdnet.com/java-zero-day-vulnerability-actively-used-in-targeted-attacks-7000003233/

FireEye
http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

AlienVault
http://labs.alienvault.com/labs/index.php/2012/new-java-0day-exploited-in-the-wild/

August 29 – UPDATED REFERENCES
Websense:

http://community.websense.com/blogs/securitylabs/archive/2012/08/28/new-java-0-day-added-to-blackhole-exploit-kit.aspx

Krebs on Security:
http://krebsonsecurity.com/2012/08/attackers-pounce-on-zero-day-java-exploit/

SecureList:
http://www.securelist.com/en/blog/208193822/The_Current_Web_Delivered_Java_0day

PCWORLD:
http://www.pcworld.com/businesscenter/article/261573/unpatched_java_vulnerability_exploited_in_blackholebased_attacks.html